NetIQ® AppManager™ 9.1
Security Target

Initial Draft Date:	February 3, 2016
Last Updated:	November 4, 2016
Version:	1.4
Prepared By:	NetIQ Corporation
Prepared For:	

NetIQ Corporation
Suite 1200
515 South Post Oak Blvd
Houston, TX 77027

Table of Contents

Figures:

Tables:

1. Security Target Introduction (ASE_INT)

This section presents the following information:

- Security Target Reference
- Target of Evaluation Reference
- TOE Overview
- CC Conformance Claims
- Specifies the Security Target conventions,
- Describes the Security Target Organization

1.1. Security Target Reference:

ST Title:	NetIQ® AppManager™ 9.1 Security Target
ST Version:	1.4
ST Date:	November 4, 2016
ST Author:	Michael F. Angelo 713-418-5396 angelom@netiq.com

1.2. Target of Evaluation Reference:

TOE Reference:	NetIQ® AppManager™ 9.1[1]
TOE Version #:	9.1.1.419
TOE Developer:	NetIQ Corporation
Evaluation Assurance Level (EAL):	EAL2+
TOE Components:	

Control Center Console	9.1.1.419
Operator Console	9.1.1.419
Security Manager Console	9.1.1.419
NetIQ Database (QDB)	9.1.1.419
Control Center Database (CCDB)	9.1.1.419
Management Server (MS)	9.1.1.419
Control Center Command Queue Service (CQS)	9.1.1.419
Task Scheduler (NQAMTS)	9.1.1.419
Deployment Servers	9.1.1.419
Control Center Deployment Web Server (CCDWS)	--[2]
Agent (NQPerfProvider4.exe)	7.9.63.0

1.3. Target of Evaluation Overview (TOE):

1.3.1. Product Overview:

The NetIQ AppManager 9.1 (AM) product delivers comprehensive systems management, including monitoring, reporting & analysis, diagnostics and resolution. It is designed to manage a variety of components – from physical hardware to server applications to end-user response time.

[1] Note: The official name of the product is: NetIQ® Application Manager™ 9.1 (Application Manager™ 9.1). The released product can be uniquely identified as: Application Manager™ 9.1.1.419 or Application Manager™ 9.1. The product name may also be abbreviated as *AppManager*™ 9.1 or simply *AppManager*, or the *TOE*. For the purpose of this certification, and the associated documentation, all of the above references are equivalent.

[2] The installer is signed by NetIQ, and contains the scripts that are used to instantiate this component at install time.

Key benefits of AppManager are:

- **Gain Greater Control over the IT Environment:**
  AppManager establishes control through features such as automated detection and deployment, policy exception management, secure delegation and self-maintaining service maps. These features help establish a solid systems management foundation so that enterprises can safely adopt and exploit next-generation technologies.
- **Improve IT Management Productivity and Visibility:**
  AppManager provides IT automation that adapts to dynamic business environments. End-to-end service visibility vastly reduces and pre-empts business service downtime and event impact assessment through visually represented service maps.
- **Maximize Return on IT Investment:**
  AppManager provides extensive out-of-the-box functionality, flexible integration with existing IT infrastructure; extensible platform and easy customization ensure that enterprises benefit from maximum functionality with the shortest time to value.

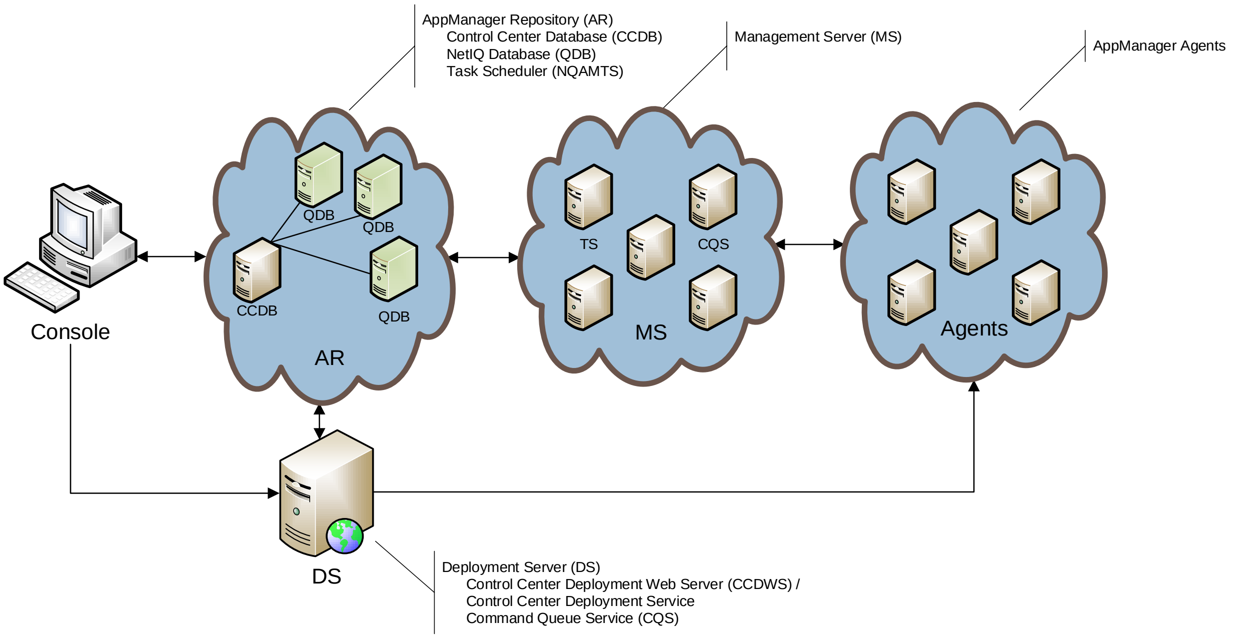
AppManager Repository (AR)
Control Center Database (CCDB)
NetIQ Database (QDB)
Task Scheduler (NQAMTS)
Management Server (MS)
AppManager Agents
QDB
QDB
QDB
CCDB
AR
Console
TS
CQS
MS
Agents
DS
Deployment Server (DS)
Control Center Deployment Web Server (CCDWS) /
Control Center Deployment Service
Command Queue Service (CQS)

Figure 1: AppManager Potential Configuration[3]

NetIQ AppManager (Figure 1[4] above) consists of the following components:

- Console machine (Console)
  - Control Center Console
  - Operator Console
  - Security Manager Console
- AppManager Repository (AR)
  - Control Center Database (CCDB)
  - NetIQ Database (QDB)

[3] Note: There can be multiple Consoles, Management Servers, and AM Agents, however for the purpose of this certification we will only be using a single configuration of each of these.

[4] Note: Only one device of each class will be used in the evaluation. Explicitly one Console, one AppManager Repository, one Management Server (MS), and one Agent.

  - Task Scheduler (NQAMTS)
- Management Server (MS)
- Deployment Server (DS)
  - Control Center Deployment Web Server (CCDWS)
  - Control Center Deployment Service (CCDS)
  - Control Center Command Queue Service (CQS)
- AppManager Agents (Agents)
  - Windows

Note that an AppManager installation always consists of one AppManager repository, at least one AppManager management server, one Operator Console or Control Center, and some number of AppManager agents on managed computers (managed clients) that report events and data through the management server to the repository. A single management site may have multiple management servers to distribute processing and communication for managed clients, but each management server communicates with only one repository.

The evaluated configuration is below:

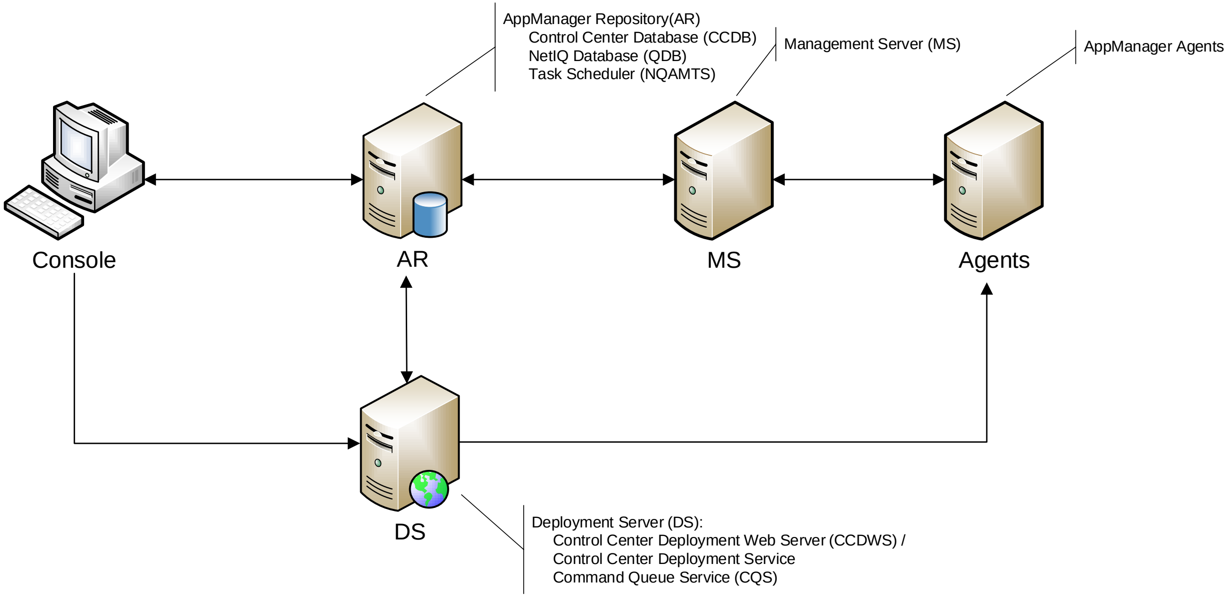
AppManager Repository(AR)
Control Center Database (CCDB)
NetIQ Database (QDB)
Task Scheduler (NQAMTS)
Management Server (MS)
AppManager Agents
Console
AR
MS
Agents
DS
Deployment Server (DS):
Control Center Deployment Web Server (CCDWS) /
Control Center Deployment Service
Command Queue Service (CQS)

Figure 2: AppManager Evaluated Configuration

1.3.2. TOE Components:

This certification covers the following AppManager Components:

- The NetIQ AppManager Console[5] application includes the following functional components:
  - Control Center Console
  - Operator Console
  - Security Manager Console

  The Control Center Console provides some additional functionality and permissions such as:
  - Performing deployment tasks
  - Checking in deployment tasks
  - Defining deployment rules

[5] We will refer to the NetIQ AppManager Console simply as Console

  - Accepting deployment tasks to push out new agents, patches and/or modules

  The Operator Console allows authorized administrators (and users) to:
  - monitor real-time events and data from a single AppManager repository (QDB)
  - allows authorized administrators (and users) to monitor real-time events and data from one or more QDBs
  - depending on the permissions granted a user may perform tasks such as:
  - creating, starting, stopping and deleting jobs
  - acknowledging, closing and deleting events
  - adding computers to and deleting computers from the AppManager repository

  The Security Manager Console allows authorized administrators the ability to:
  - control access to views in the Operator Console
  - control tasks in the Operator Console
  - manage application or computer specific security information (i.e. SNMP community strings and passwords)

- The AppManager Repository – consists of a Control Center Database (CCDB) and the NetIQ Database (QDB). The Repository is used to store:
  - configuration information
  - knowledge scripts and managed objects that can be used to provide tasks for the agents
  - The Task scheduler (NQAMTS) (also on the MS) is responsible for coordinating data between QDBs.
- The Management Server is responsible for communicating:
  - data and events between the NetIQ AppManager Agent and the AppManager Repository
  - sending NetIQ AppManager jobs to the NetIQ AppManager agent from the AppManager Repository
- The **Deployment Server** consists of two pieces – the NetIQ AppManager Control Center Deployment Service and the NetIQ AppManager Control Center Deployment Web Server.
  - **The NetIQ AppManager Control Center Deployment Service** application installs AppManager agents, AppManager agent patches and AppManager modules on targeted IT systems. The Control Center Deployment Service periodically evaluates deployment rules stored in the Control Center database to see if there are eligible targeted IT systems that need agents, patches or modules installed on them. If a deployment rule matches a targeted IT system the Control Center Deployment Service gets the install packages from the NetIQ AppManager Control Center Deployment Web Server and executes these install packages on the targeted IT system.
  - **The NetIQ AppManager Control Center Deployment Web Server** application is a Web Service that provides installation packages to the AppManager Control Center Deployment Service.
  - The CQS, housed on the MS, synchronizes the CCDB and the QDB. In addition the NQAMTS keeps track of the administrative database tasks and invokes them.
- The Agent consists of components running on targeted IT systems. These agents send collected data and events to the NetIQ AppManager Management Server in real-time.

  NetIQ agents gather data values for specified metrics and/or compare these values to specified thresholds on a scheduled basis. These parameters are defined in NetIQ AppManager Knowledge Scripts (KS). An instance of a running KS is an AppManager job. In a standard agent-based configuration, there is a NetIQ client application called an agent running on the same machine as the targeted IT system.

In a proxy agent configuration, there is no TOE software running on the targeted IT system. The TOE in a proxy agent configuration uses targeted IT system-specific interfaces (e.g. Application-specific network interfaces, etc.) to collect data and events. In the event of a data value crossing a threshold the agent generates an event and executes any associated actions. Actions can be things such as running a script or batch file, issuing an SNMP trap, sending an email, writing to an event log, etc.

1.3.3. Major Security Features of the TOE:

The TOE provides the ability to:

- Collect and react to events from targeted IT systems using administrator defined AppManager Knowledge Scripts
- Collect and archive collected data from targeted IT systems
- Generate reports to review collected data.

The TSF provides the following security functions:

- Security Audit
- User Data Protection
- Identification and Authentication
- Security Management

1.3.3.1. Security Audit

The TOE can be set up to produce transaction audit reports for job / event related operations and to aid in their analysis via the use of the Console. The TOE reporting capabilities are completely configurable.

1.3.3.2. User Data Protection

The TOE implements multiple levels of access as well as functions to enforce them. Jobs can be executed, knowledge scripts can be imported and exported from the TOE as well as moved across different components in the TOE. Inter-TSF data confidentiality transfers are protected by use of the Operating Environments native communications process.

1.3.3.3. Identification and Authentication

The TOE maintains authorization information that determines which TOE functions an authenticated administrator or user (or a given role) may perform. The TOE maintains its own set of credentials for Agents, groups of agents, administrators and users assigned to each of those groups and agents. In addition the TOE validates that users are members of the appropriate groups prior to performing tasks. This information is maintained in the QDB. The TOE depends on the IT Environment for protection of passwords and service credentials, as well as for user authentication, identification, and subject binding[6]

1.3.3.4. Security Management

Security functions and attributes in the TOE are controlled / managed and specified at different levels or roles by the TSF and the IT Environment. The TOE and IT Environment can also be used to revoke individual access.

1.3.4. TOE TYPE:

For the purpose of this security target the TOE Type is a **W**indows **M**anagement **Performance P**roxy (WMPP).

1.3.5. Non-TOE hardware/software/firmware required by the TOE:

[6] (tieing users to actions)

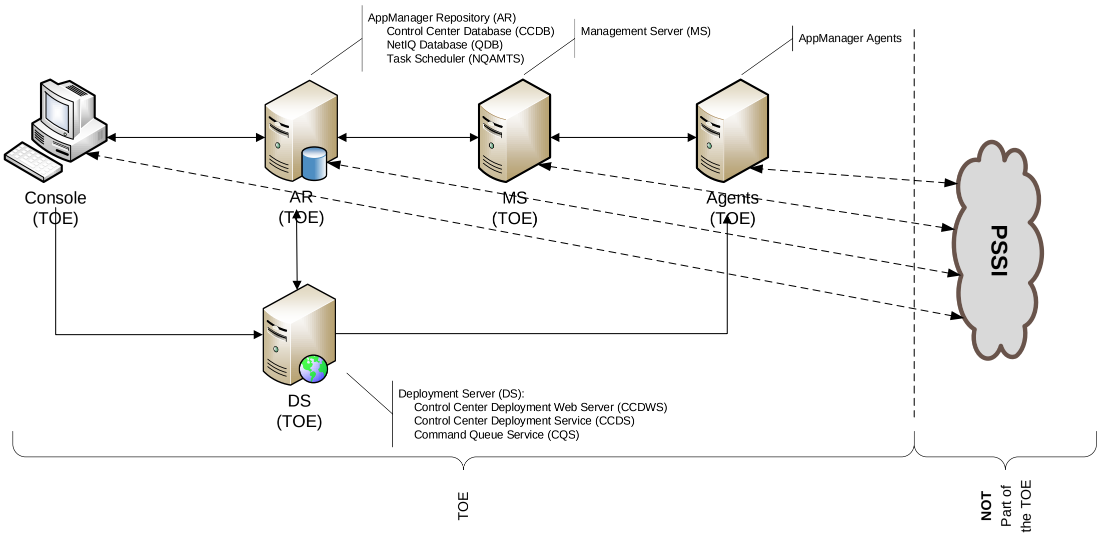

Figure 3: NetIQ AppManager Configuration

All elements in Figure 3, labeled (TOE) are covered by this ST.

While the TOE runs on numerous operating systems and versions of them, we are only listing the operating systems and versions that will be used in this test. For a complete list of supported operating systems and versions please refer to the Installation Guide.

In addition the system requires a network which may consist of routers, switches, hubs, and other technology used in a TCP/IP based network, which are also not part of the TOE.
For those components that are resident on a Microsoft Operating System, the encryption technology is provided natively by Microsoft as part of the operating environment.

The system will also require SQL server as a database component, which is provided by a third party, and is not part of the TOE.

Finally the system may employ SSL, MSMQ, DCOM, and .net Remoting for communications, which are provided by a third party and are not part of the TOE.

The operating system environment(s) is responsible for providing FIPS 140-2 Validated encryption.

1.3.6. Evaluated Configuration

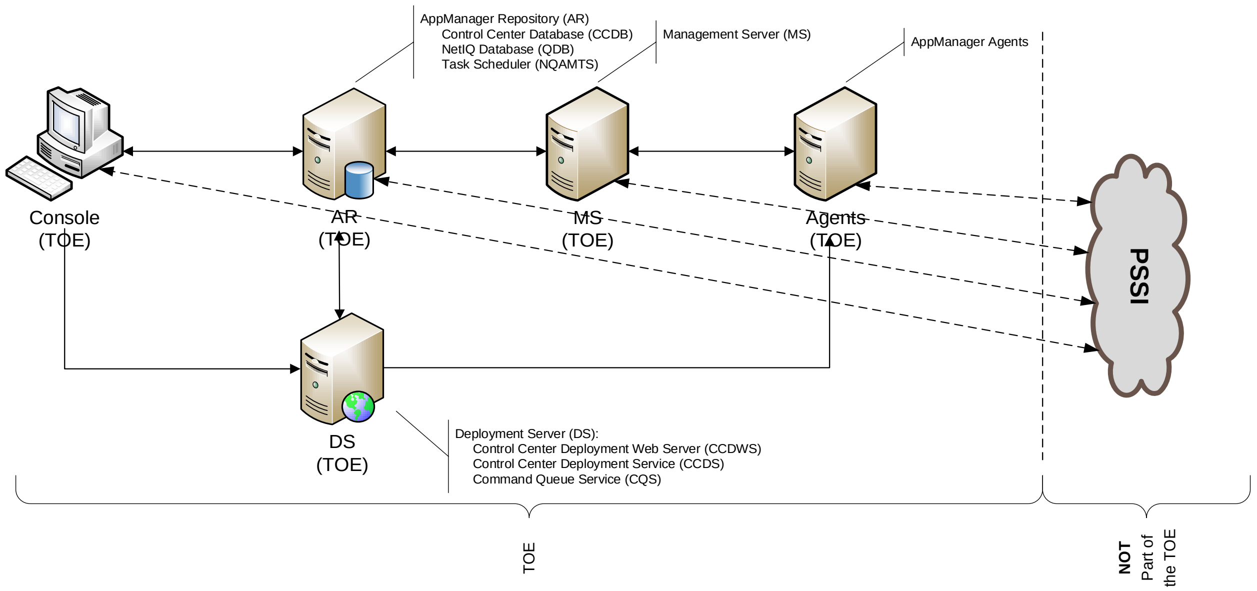

Figure 4: Evaluated Configuration

1.3.7. Physical Scope of TOE

The NetIQ AppManager program is a software only TOE. The TOE consists of the elements in Figure 4 (above), labeled (TOE). The TOE explicitly includes at least one Console, CCDB/QDB/CQS, MS, CCDWS, CCDS, and at least one Client all running on at least one of their supported operating systems. The TOE explicitly excludes the Professional Services Support Interface (PSSI).

User installation and guidance documents are supplied with the TOE. They are:

- Administrator Guide
  NetIQ® AppManager®
  April 2016
- Control Center User Guide
  NetIQ® AppManager®
  April 2016
- Installation Guide
  NetIQ® AppManager®
  April 2016
- NetIQ® AppManager®
  Upgrade and Migration Guide
  June 20 2016
- AppManager Operator Console User Guide
  NetIQ® AppManager®
  March 2007

The components that make up the evaluated configuration are:

- Console
- AppManager Repository
- Management Server
- Managed Client(s)
- Deployment Server

The Console will be evaluated on the following operating systems:

- Windows 8.1

The AppManager Repository will be evaluated in the consolidated configuration with the following operating systems:

- Microsoft Windows Server 2012 R2

The Management Server will be evaluated on the following operating systems:

- Microsoft Windows Server 2012 R2

The Agents will be evaluated on the following operating systems:

- Microsoft Windows Server 2012 R2

The Control Center Deployment Server will be evaluated on the following operating systems:

- Microsoft Windows Server 2012 R2

1.4. Security Target Conventions:

This section specifies the formatting information used in the ST. The notation, conventions, and formatting in this security target are consistent with Version 3.1 of the Common Criteria for Information Security Evaluation. Clarifying information conventions, as well as font styles were developed to aid the reader.

- Security Functional Requirements – Part 1, section C.2 of the CC defines the approved set of operations that may be applied to functional requirements: assignment, iteration, refinement, and selection.
    - Assignment: allows the specification of an identified parameter or parameter(s).
    - Iteration: allows a component to be used more than once with varying operations.
    - Refinement: allows the addition of details.
    - Selection: allows the specification of one or more elements from a list.
- Within section 6 of this ST the following conventions are used to signify how the requirements have been modified from the CC text.
    - Assignments are indicated using bold and are surrounded by brackets (e.g., **[assignment**]).
    - Iteration is indicated by a letter placed at the end of the component. For example FDP_ACC.1a and FDP_ACC.1b indicate that the ST includes two iterations of the FDP_ACC.1 requirement, a and b.
    - Refinements are indicated using bold, for additions, and strike-through, for deletions (e.g., "… **every** object …" or "… ~~all~~ **things** …").
    - Selections are indicated using italics and are surrounded by brackets (e.g., [*selection*]).
- Other sections of the ST – Other sections of the ST use bolding to highlight text of special interest, such as acronyms, definitions, or captions.

1.5. Acronyms:

AD	Active Directory
AM	AppManager
API	Application programming interface
AR	AppManager Repository
CC	Common Criteria
CCDB	Control Center Database
CCDS	Control Center Deployment Service
CCDWS	Control Center Deployment Web Server
CCEVS	Common Criteria Evaluation and Validation Scheme
CEM	Common Evaluation Methodology
CQS	Command Queuing Services
EAL	Evaluation Assurance Level
FIPS	Federal Information Processing Standards
GUI	Graphical User Interface
HLD	High-level Design
IA	Initial Assessment
IDS	Intrusion Detection Systems
MS	Management Server
NSS	Network Security System
NIAP	National Information Assurance Partnership
NIST	National Institute of Standards and Technology
NQAMTS	NetIQ AM Task Scheduler
NSA	National Security Agency
OS	Operating system
PP	Protection Profile
PSSI	Professional Services Support Interface
QDB	NetIQ Database
SMTP	Simple Mail Transport Protocol
SNMP	Simple Network Monitoring Protocol
SOF	Strength of Function
SSL	Secure Socket Layer
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functionality
TSP	TOE Security Policy
UI	User Interface
WMPP	Windows Management Performance Proxy

1.6. Security Target Organization

The Security Target (ST) contains the following sections:

Section 1	Security Target Introduction (ASE_INT)	The ST introduction describes the Target of Evaluation (TOE) in a narrative with three levels of abstraction: A TOE reference, TOE overview, a TOE description (in terms of physical and logical boundaries) and scoping for the TOE.
Section 2	CC Conformance Claims (ASE_CCL)	This section details any CC and PP conformance claims.
Section 3	Security Problem (ASE_SPD)	This section summarizes the threats addressed by the TOE and assumptions about the intended environment.
Section 4	Security Objectives (ASE_OBJ)	This section provides a concise statement in response to the security problem defined in definition.
Section 5	Extended Components Definition (ASE_ECD)	This section provides information about security requirements outside of components described in CC Part 2 or CC Part 3.
Section 6	IT Security Requirements (ASE_REQ)	This section provides a description of the expected security behavior of the TOE.
Section 7	TOE Summary Specification (ASE_TSS)	This section provides a general understanding of the TOE implementation.

1.7. Functionality excluded from the Certification

The operating system environment is responsible for providing encryption.

In addition while the network environment will be tested using OpenSSL, OpenSSL will not be included in the functional testing.

Finally, the product supports agents on *ix (UNIX, Linux) which are also not included in the certification.

2. CC Conformance Claims (ASE_CCL)

2.1. CC Conformance Claims

This TOE is conformant to the following CC specifications:

- Common Criteria for Information Technology Security Evaluation Part 2: Security Functional Requirements, Version 3.1 Release 4, September 2012. Part 2 Extended
- Common Criteria for Information Technology Security Evaluation Part 3: Security Assurance Requirements, Version 3.1 Release 4, September 2012. Part 3 Conformant
- The TOE is augmented with ALC_FLR.1 Basic Flaw remediation.
- The Evaluation Assurance Level (EAL) is 2+ (EAL2+)

2.2. PP Claim

The TOE does not claim conformance to any Protection Profiles (PPs).

2.3. Package Claim

The TOE claims conformance to the EAL2 assurance package defined in Part 3 of the Common Criteria Version 3.1 Revision 4 (September 2012). The TOE does not claim conformance to any functional package.

2.4. Conformance Rationale:

No conformance rationale is necessary for this evaluation since this Security Target does not claim conformance to a Protection Profile.

3. Security Problem (ASE_SPD)

This section summarizes the threats addressed by the TOE and assumptions about the intended environment of the TOE. Note that while the identified threats are mitigated by the security functions implemented in the TOE, the overall assurance level (EAL2+) also serves as an indicator of whether the TOE would be suitable for a given environment.

3.1. Introduction:

In order to simplify the security problem, the TOE can be broken into 3 areas. These areas are the:

Assets	elements of the TOE that need protections
Subjects	persons with legitimate access to the TOE
Attackers	persons that are not a legitimate users

3.1.1. Assets:

The assets can be broken down into two classes – Primary and Secondary. The main aim of this TOE is to protect the primary assets against unauthorized access, manipulation, and disclosure. The primary assets are:

- Data stored on the AppManager Repository (CCDB, QDB)
- Configuration information stored on the AppManager Repository, Console, Agents, Control Center Deployment Server.
- Data in transit from / to the Agents, AppManager Repository, Console, and the Control Center Deployment Server

The Secondary assets are themselves of minimal value, the possession of these assets enables or eases access to primary assets. Therefore these assets need to be protected as well.

- Credentials (i.e. account information and associated passwords) for access to the TOE
- Security attributes (i.e. File access permissions) on the TOE.
- Explicit Product privileges afforded to users of the TOE.

3.1.2. Subjects:

Subjects have privileges and associations depending on their roles in the AppManager infrastructure. Finally credentials for Agents are also provided. In addition all credentials and authorization associations are stored in the QDB. A more detailed description of the different privileges can be found in Appendix A.

3.1.2.1. Administrators:

AppManager administrators can perform tasks associated with adding users, agents, or groups to the infrastructure. In addition they can assign default privileges for tasks to be executed on groups of machines. Administrators can also define group machine classes (which consist of groups of agents.) Finally administrators can place users into groups (or classes) of machines.

3.1.2.2. AM Users:

Can view data, start and stop jobs, define new jobs for groups of machines.

3.1.2.3. AM Agents:

Agents return data and event notifications from jobs running on machines.

3.1.3. Attacker:

An Attacker is a person (or persons) who is not a user or administrator, and has not physical access to any device in the infrastructure. This means that their only mode of access would be from outside the corporate environment (i.e. a machine on the Internet).

A successful attacker would be able to gain access to TOE resources. Assuming successful access that attacker would then attempt to:

- access the console as an authorized user create / modify / delete jobs
- access the AppManager Repository and create / modify / delete jobs or data

- delete all data in the AppManager Repository
- access the Deployment Server and deploy packages
- access the agents and provide erroneous data to the AppManager Repository

3.2. Assumptions

3.2.1. Intended Usage Assumptions

A.ACCESS The TOE has access to all the IT System data it needs to perform its functions.

A.DYNMIC The TOE will be managed in a manner that allows it to appropriately address changes in the IT System the TOE monitors.

A.ASCOPE The TOE is appropriately scalable to the IT System the TOE monitors.

3.2.2. Physical Assumptions

A.LOCATE The server components of the TOE will be located within controlled access facilities, which will prevent unauthorized physical access.

A.AUTHCON The TOE will be able to rely on the IT environment to determine the identity of users.

A.ENVFAC The TOE will be able to rely on the IT environment to obtain a reliable time stamp.

3.2.3. Personnel Assumptions

A.MANAGE There will be one or more competent individuals assigned to manage the TOE and the security of the information it contains.

A.NOEVIL The authorized administrators are not careless, willfully negligent, or hostile, and will follow and abide by the instructions provided by the TOE documentation.

3.2.4. Connectivity Assumptions:

A.AVAIL The systems, networks and all components will be available for use.

A.CONFIG The systems will be configured to allow for proper usage of the application.

A.NETCON All networks will allow for communications between the components.

3.3. Threats

3.3.1. Threats to the TOE

T.ADMIN_ERROR An authorized administrator may incorrectly install or configure the TOE resulting in ineffective security mechanisms.

T.MAL_INTENT An authorized user could initiate changes that grant themselves additional unauthorized privileges.

T.MIS_NORULE Unauthorized accesses and activity, indicative of misuse, may occur on an IT System the TOE is installed on and the TOE response may not occur if no event rules are specified in the TOE.

T.NO_HALT An unauthorized entity may attempt to compromise the continuity of the TOE by halting execution of the TOE or TOE Components.

T.PRIV An unauthorized entity may gain access to the TOE and exploit functionality to gain access or privileges to TOE security functions and data.

T.TSF_COMPROMISE A malicious user may cause configuration data to be inappropriately accessed (viewed, modified or deleted).

T.SC_MISCFG Improper security configuration settings may exist in the IT System the TOE is on and could make the TOE audit ineffective.

T.SC_MALRUN Users could execute malicious code on an IT System that the TOE is installed on which causes modification of the TOE protected data or undermines the IT System security functions.

4. Security Objectives (ASE_OBJ)

4.1. Security Objectives for the TOE

O.ADMIN_ROLE The TOE will define authorizations that determine the actions authorized administrator roles may perform.

O.MANAGE The TOE will allow administrators to effectively manage the TOE and its security functions,

O.OFLOWS The TOE must appropriately handle potential System data storage overflows.

O.RESPONSE The TOE must respond appropriately to trigger events.

O.AM_AUTH The TOE must ensure that only authorized administrators are able to access functionality.

O.AM_AUDIT The TOE must collect and store transactional information that can be used to audit jobs, data, or events.

O.AM_ACPOL The TOE must provide an access policy.

4.2. Security Objectives for the Non-IT Environment

OE.INSTAL Those responsible for the TOE must ensure that the TOE is delivered, installed, managed, and operated in a manner which is consistent with IT security.

OE.CREDEN Those responsible for the TOE must ensure that all access credentials are protected by the users in a manner which is consistent with IT security.

OE.PERSON Personnel working as authorized administrators shall be carefully selected and trained for proper operation of the System.

OE.PHYCAL Those responsible for the TOE must ensure that those parts of the TOE critical to security policy are protected from any physical attack.

OE.INTROP The TOE is interoperable with the Environment it manages.

4.3. Security Objectives for the IT Environment

OE.USER_AUTHENTICATION The IT environment will verify the claimed identity of users.

OE.USER_IDENTIFICATION The IT environment will uniquely identify users.

OE.TIME The IT environment will provide a time source that provides reliable time stamps.

OE.TOE_PROTECTION The IT Environment will protect the TOE and its assets from external interference or tampering.

4.4. Rationale

This section provides the rationale for completeness and consistency of the Security Target. The rationale addresses the following areas:

- Security Objectives;
- Security Functional Requirements;
- Security Assurance Requirements;

- ○ Requirement Dependencies;
- ○ TOE Summary Specification; and,
- ○ PP Claims

4.5. Security Objectives Rationale

This section shows that all secure usage assumptions, organizational security policies, and threats are completely covered by security objectives. In addition, each objective counters or addresses at least one assumption, organizational security policy, or threat.

4.5.1. Security Objectives Rationale for the TOE and Environment

This section provides evidence demonstrating the coverage of threats by the security objectives.

		O.ADMIN_ROLE	O.MANAGE	O.OFLOWS	O.RESPONSE	O.AM_ACPOL	O.AM_AUTH	O.AM_AUDIT	OE.TOE_PROTECTION
Threats to the TOE	T.ADMIN_ERROR		X						
	T.MAL_INTENT			X	X	X		X	X
	T.MIS_NORULE					X		X	
	T.NO_HALT	X			X				
	T.PRIV	X						X	
	T.TSF_COMPROMISE								X
	T.SC_MISCFG					X	X	X	
	T.SC_MALRUN	X					X	X	

Table 1: Environment to Objective Correspondence

4.5.1.1. T.ADMIN_ERROR

An authorized administrator may incorrectly install or configure the TOE resulting in ineffective security mechanisms.

This Threat is countered by ensuring that:

O.MANAGE: The TOE counters this threat by providing a user interface that allows Administrators to effectively manage the TOE and its security functions. In addition the TOE ensures that only authorized entities are able to access such functionality.

4.5.1.2. T.MAL_INTENT:

An authorized user could initiate changes that grant themselves additional unauthorized privileges.

This Threat is countered by ensuring that:

O.OFLOWS: The TOE counters this by preventing transactions from occurring when the system runs out of storage space..

O.RESPONSE: The TOE counters this event by responding appropriately to trigger events.

O.AM_ACPOL: The TOE counters this threat by providing an access policy.

O.AM_AUDIT: The TOE counters this event by collecting and storing transactional information that can be used to audit changes to the AD.

OE.TOE_PROTECTION: The IT Environment counters this threat by protecting the TOE and its assets from external interference or tampering.

4.5.1.3. T. MIS_NORULE

Unauthorized accesses and activity, indicative of misuse, may occur on an IT System the TOE is installed on and the TOE response may not occur if no rules are specified in the TOE.
This Threat is countered by ensuring that:

O.AM_AUDIT: The TOE collects and stores transactional information that can be used to audit changes to the AD.

O.AM_ACPOL: The TOE protects against this threat by providing access policies.

4.5.1.4. T.NO_HALT:

An unauthorized entity may attempt to compromise the continuity of the TOE by halting execution of the TOE or TOE Components.

This Threat is countered by ensuring that:

O.ADMIN_ROLE: The TOE counters this threat by defining authorizations that determine the actions authorized entities may perform.

O.RESPONSE: The TOE defines triggers that can be used to notify of events. This threat can be mitigated by configuring a trigger when a shutdown is attempted.

4.5.1.5. T.PRIV:

An unauthorized entity may gain access to the TOE and exploit functionality to gain access or privileges to TOE security functions and data.
This Threat is countered by ensuring that:

O.ADMIN_ROLE: The TOE counters this threat by providing strict access controls which determine the actions / roles authorized assistant administrators may perform.

O.AM_AUDIT: The TOE counters this threat by providing transactional based audit capabilities.

4.5.1.6. T.TSF_COMPROMISE

A malicious user may cause configuration data to be inappropriately accessed (viewed, modified or deleted).
This Threat is countered by ensuring that:

OE.TOE_PROTECTION: The IT environment will protect the TOE and its assets from external interference or tampering.

4.5.1.7. T. SC_MISCFG

Improper security configuration settings may exist in the IT System the TOE is on and could make the TOE audit ineffective.
This Threat is countered by ensuring that:

O.AM_AUTH: The TOE protects against this threat by ensuring that only authorized administrators are able to access functionality.

O.AM_ACPOL: The TOE counters this threat by providing an access policy.

O.AM_AUDIT: The TOE counters this threat by providing transactional based audit capabilities.

4.5.1.8. T. SC_MALRUN

Users could execute malicious code on an IT System that the TOE is installed on which causes modification of the TOE protected data or undermines the IT System security functions.
This Threat is countered by ensuring that:

O.ADMIN_ROLE: The TOE counters this threat by defining authorizations that determine the actions / roles that authorized entities may perform.

O.AM_AUTH: The TOE protects against this threat by ensuring that only authorized administrators are able to access functionality.

O.AM_AUDIT: The TOE counters this threat by providing transactional based audit capabilities.

4.6. Security Objectives Rationale for Environment Assumptions

This section provides evidence demonstrating coverage of the Non-IT security objectives by the environmental assumptions. The following table shows this assumption to objective mapping.

		OE.INSTAL	OE.CREDEN	OE.PERSON	OE.PHYCAL	OE.INTROP	OE.USER_AUTHENTICATION	OE.USER_IDENTIFICATION	OE.TIME
Intended usage assumptions	A.ACCESS					X			
	A.ASCOPE					X			
	A.DYNMIC			X		X			
Physical assumptions	A.LOCATE				X				
	A.AUTHCON						X	X	
	A.ENVFAC								X
Personnel assumptions	A.MANAGE			X					
	A.NOEVIL	X	X						
Connectivity assumptions	A.AVAIL				X	X			
	A.CONFIG				X	X			
	A.NETCON				X	X			

Table 2: Complete coverage – environmental assumptions

4.6.1. A.ACCESS

The TOE has access to all the IT System data it needs to perform its functions.

This Assumption is satisfied by ensuring that:

OE.INTROP: The OE.INTROP objective ensures the TOE has the needed access.

4.6.2. A.ASCOPE

The TOE is appropriately scalable to the IT System the TOE monitors.

This Assumption is satisfied by ensuring that:

OE.INTROP: The OE.INTROP objective ensures the TOE has the necessary interactions with the IT System it monitors.

4.6.3. A.DYNMIC

The TOE will be managed in a manner that allows it to appropriately address changes in the IT System the TOE monitors.

This Assumption is satisfied by ensuring that:

OE.PERSON: The OE.PERSON objective ensures that the TOE will be managed appropriately.

OE.INTROP: The OE.INTROP objective ensures the TOE has the proper access to the IT System.

4.6.4. A.AUTHCON

The TOE will be able to rely on the IT environment to determine the identity of users.
This Assumption is satisfied by ensuring that:

OE.USER_AUTHENTICATION The OE.USER_AUTHENTICATION ensures that the IT environment can verify the claimed identity of users.

OE.USER_IDENTIFICATION The OE.USER_IDENTICATION ensures that the IT environment can uniquely identify users.

4.6.5. A.ENVFAC

The TOE will be able to rely on the IT environment to obtain a reliable time stamp.
This Assumption is satisfied by ensuing that:

OE.TIME The OE.TIME ensures that the IT environment will provide a time source to be used for reliable time stamps.

4.6.6. A.LOCATE

The server components of the TOE will be located within controlled access facilities, which will prevent unauthorized physical access.
This Assumption is satisfied by ensuring that:

OE.PHYCAL: The OE.PHYCAL provides for the physical protection of the TOE.

4.6.7. A.MANAGE

There will be one or more competent individuals assigned to manage the TOE and the security of the information it contains.
This Assumption is satisfied by ensuring that:

OE.PERSON: The OE.PERSON objective ensures all authorized administrators are qualified and trained to manage the TOE.

4.6.8. A.NOEVIL

The authorized administrators are not careless, willfully negligent, or hostile, and will follow and abide by the instructions provided by the TOE documentation.

This Assumption is satisfied by ensuring that:

OE.INSTAL: The OE.INSTAL objective ensures that the TOE is properly installed and operated.

OE.CREDEN: The OE.CREDEN objective supports this assumption by requiring protection of all authentication data

4.6.9. A.AVAIL

The IT environment will be available for use by the TOE.

OE.PHYCAL: The OE.PHYCAL objective ensures that the TOE is in a protected environment.

OE. INTROP: The OE.INTROP objective ensures that the TOE can interoperate with the environment it is deployed in.

4.6.10. A.CONFIG

The IT environment is properly configured for use by the TOE.

OE.PHYCAL: The OE.PHYCAL objective ensures that the TOE configuration is properly protected.

OE. INTROP: The OE.INTROP objective ensures that the TOE is configured to properly interoperate with the environment it is deployed in.

4.6.11. A.NETCON

The IT network environment is properly protected and can be used by the TOE.

OE.PHYCAL: This objective provides for the physical protection of the TOE Network and Network Elements. .

OE. INTROP: The OE.INTROP objective ensures that the network interface is configured to properly interoperate with the environment and the TOE.

4.7. Security Requirements Rationale

This section demonstrates how there is at least one functional component for each TOE security objective (and how all SFRs map to one or more TOE security objectives) by a discussion of the coverage for each TOE security objective.

	O.ADMIN_ROLE	O.MANAGE	O.OFLOWS	O.RESPONSE	O.AM_ACPOL	O.AM_AUTH	O.AM_AUDIT
FAU_ARP.1				X			
FAU_GEN.1							X
FAU_SAA.1				X			
FAU_SAR.1							X
FAU_STG.1							X
FDP_ACC.1					X	X	
FDP_ACF.1					X	X	X
FIA_ATD.1	X						
FMT_MOF.1		X					x
FMT_MSA.1						X	
FMT_MSA.3						X	
FMT_MTD.1		X					x
FMT_SMF.1		X					x
FMT_SMR.1	X				X		
WMPP_ADM.1 (EX)	X	X					
WMPP_ALR.1 (EX)			X	X			

WMPP_STG.1(EX)			X				

Table 3: Objective to Requirement Correspondence

4.7.1. O.ADMIN_ROLE

The TOE will define authorizations that determine the actions authorized administrator roles may perform.

This TOE Security Objective is satisfied by ensuring that:

FIA_ATD.1: The TOE maintains authorization information that determines which TOE functions a role may perform.

FMT_SMR.1: The TOE recognizes any user account that is assigned in the IT environment to one or more system-defined operating system user groups “Authorized Administrator”.

WMPP_ADM.1(EX) The TOE defines a mechanism where Administrators can delegate to authorized users the capability to issue administrative commands and changes

4.7.2. O.MANAGE

The TOE will allow administrators to effectively manage the TOE and its security functions, and must ensure that only authorized administrators are able to access such functionality.

This TOE Security Objective is satisfied by ensuring that:

FMT_MOF.1: The TOE restricts the ability to manage WMPP settings to authorized administrators or users with privileges specified in Appendix A.

FMT_MTD.1: The TOE restricts the ability to query collected data and generated reports to authorized users.

FMT_SMF.1: The TOE provides authorized administrators with the ability to manage WMPP settings and review collected data and correlation reports.

WMPP _ADM.1(EX): The TOE provides authorized administrators with the ability to delegate to privileges to individuals to create, delete or modify activities that take place on managed clients.

4.7.3. O. OFLOWS

The TOE must appropriately handle potential System data storage overflows.

This TOE Security Objective is satisfied by ensuring that:

WMPP_ALR.1(EX): The TOE generates an event failure alarm (message) when audit storage space is exceeded.

WMPP_STG.1 (EX): The TOE stops transactions from occurring when audit storage space is exceeded. Failed attempts due to storage generate messages.

4.7.4. O. RESPONSE

The TOE must respond appropriately to event triggers

This TOE Security Objective is satisfied by ensuring that:

FAU_ARP.1: The TOE can be configured to generate event triggers and be programmed to respond to those events.

FAU_SAA.1: The TOE can be configured to look at an events occurrence and generate an alarm.

WMPP _ALR.1(EX): The TOE generates alarms (called actions) that notify authorized administrators or assistants using the console, using email, using SMTP, and/or executing a command in a configured script. Note that alarms may be generated in response to administratively-configured processing rules.

4.7.5. O.AM_ACPOL

The TOE must provide an access policy.

FDP_ACC.1: The TOE can be configured to limit access to Administrators, AM Users and AM Agents.

FMT_SMR.1: The TOE recognizes any user account that is assigned in the IT environment to one or more system-defined operating system user groups “Administrators”, AM Users, or AM Agents.

FDP_ACF.1 The TOE can be configured to enforce access controls to objects.

4.7.6. O.AM_AUTH

The TOE must ensure that only authorized administrators, users, and agents are able to access the TOE functionality.

FDP_ACC.1: The TOE can be configured to limit access to Administrators, AM Users, and AM Agents.

FDP_ACF.1: The TOE can be configured to enforce access controls to objects.

FMT_MSA.1: The TOE will enforce access controls that restrict the ability to alter security attributes to Administrators.

FMT_MSA.3: The TOE will enforce a default set of privileges as well as allowing Administrators to change the default set of privileges.

4.7.7. O.AM_AUDIT

The TOE must collect and store transactional information that can be used to audit jobs, data, or events.

FAU_GEN.1: The TOE provides the ability to generate audit records.

FAU_SAR.1: The TOE provides authorized users the capability to read all audit information.

FAU_STG.1: The TOE provides the ability to protect the audit record.

FDP_ACF.1: The TOE provides audit records for All requested changes by Administrators, AM Users, or Agents.

FMT_MOF.1: The TOE restricts the ability to manage WMPP settings to Administrators or users with privileges specified in Appendix A.

FMT_MTD.1: The TOE restricts the ability to add AM Users or AM Agents to Administrators.

FMT_SMF.1: The TOE generates audit records for actions performed by AM Users, AM Agents, or Administrators.

4.8. Security Assurance Requirements Rationale

EAL2+ was chosen to provide a low level of assurance that is consistent with good commercial practices. As such minimal additional tasks are placed upon the vendor assuming the vendor follows reasonable software engineering practices and can provide support to the evaluation for design and testing efforts. The chosen assurance level is appropriate with the threats defined for the environment. While the System may monitor a hostile environment, it is expected to be in a non-hostile position and embedded in or protected by other products designed to address threats that correspond with the intended environment. At

EAL2+, the System will have incurred a search for obvious flaws to support its introduction into the non-hostile environment.

The ALC_FLR.1 augmentation was claimed since fault level remediation is important to the customers of the product.

4.8.1. Requirement Dependency Rationale

The following table demonstrates that all dependencies among the claimed security requirements are satisfied and therefore the requirements work together to accomplish the overall objectives defined for the TOE.

SFR	Dependencies	Met By
FAU_ARP.1	FAU_SAA.1	Included
FAU_GEN.1	FPT_STM.1	Met by OE.TIME
FAU_SAA.1	FAU_GEN.1	Included
FAU_SAR.1	FAU_GEN.1	Included
FAU_STG.1	FAU_GEN.1	Included
FDP_ACC.1	FDP_ACF.1	Included
FDP_ACF.1	FDP_ACC.1, FMT_MSA.3	Included
FIA_ATD.1	None	None
FMT_MOF.1	FMT_SMR.1, FMT_SMF.1	Included
FMT_MSA.1	FDP_ACC.1, FMT_SMR.1, FMT_SMF.1	Included
FMT_MSA.3	FMT_MSA.1, FMT_SMR.1	Included
FMT_MTD.1	FMT_SMR.1, FMT_SMF.1	Included
FMT_SMF.1	None	None
FMT_SMR.1	FIA_UID.1	Met by OE.USER_IDENTIFICATION
WMPP_ADM.1(EX)	None	None
WMPP _ALR.1(EX)	None	None
WMPP_STG.1(EX)	None	None

Table 4: Requirement Dependency

4.9. Explicitly Stated Requirements Rationale

A class of WMPP requirements was created to specifically address the administrative proxy capability of a WMPP. The purpose of this class of requirements is to address the unique functionality of WMPP's including capabilities for making, reviewing, and managing administrative changes. These requirements have no dependencies since the stated requirements embody all the necessary security functions, with the exception of time stamps provided by the IT environment to support event correlation.

4.10. TOE Summary Specification Rationale

Each subsection in the TSS describes a security function of the TOE. Each description is followed with rationale that indicates which requirements are satisfied by aspects of the corresponding security function. The set of security functions works together to satisfy all of the security functions requirements. Furthermore, all of the security functions are necessary in order for the TSF to provide the required security functionality.

This Section in conjunction with Section 6, the TOE Summary Specification, provides evidence that the security functions are suitable to meet the TOE security requirements. The collection of security functions work together to provide all of the security requirements. The security functions described in the TOE summary specification are all necessary for the required security functionality in the TSF. Table 7 demonstrates the relationship between security requirements and security functions.

SFRs	TOE Security Functions			
	Security Audit	User Data Protection	Identification and Authentication	Security Management
FAU_ARP.1	X			
FAU_GEN.1	X			
FAU_SAA.1	X			
FAU_SAR.1	X			
FAU_STG.1	X			
FDP_ACC.1		X		
FDP_ACF.1	X	X		
FIA_ATD.1		X	X	
FMT_MOF.1				X
FMT_MSA.1				X
FMT_MSA.3				X
FMT_MTD.1				X
FMT_SMF.1				X
FMT_SMR.1			X	X
WMPP_ADM.1(EX)	X	X		
WMPP_ALR.1(EX)	X			X
WMPP_STG.1(EX)	X			X

Table 5: Security Functions vs. Requirements Mapping

5. Extended Components Definition (ASE_ECD)

This chapter defines a new class required by Windows Management Performance Proxy functionality called WMPP. The class consists of the following family members WMPP_ADM, WMPP _ALR, and WMPP_STG. This class is defined because the Common Criteria (Part 2 and Part 3) does not contain any SFRs which cover these functions. The families in this class address requirements for data review, alarms, and loss prevention.

Class	Component
WMPP: Windows Management Performance Proxy	WMPP_ADM.1(EX): Data Review
	WMPP _ALR.1(EX): Data Alarms
	WMPP_STG.1(EX): Data Loss Prevention

Table 6: Extended Functional Components

5.1. Definition for WMPP_ADM.1 (EX)

For the TOE described in this ST it was necessary to provide authorized entities with a mechanism to read and perform administrative functions as authorized. This mechanism is covered by the WMPP_ADM family and contains the components as shown in Figure 5 below.

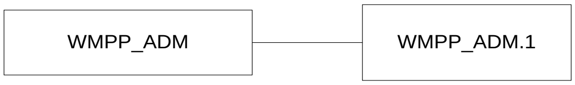

Figure 5: WMPP_ADM Component Leveling

5.1.1. Data Review (WMPP _ADM.1 (EX))

WMPP_ADM.1.1 Defines a mechanism whereby administrators can delegate to authorized users the capability to issue administrative commands and changes.

WMPP_ADM.1.2 Defines a mechanism whereby administrators can delegate to authorize users a group or set of abilities.

5.1.2. Dependencies:

- None

5.1.3. Management:

- None

5.2. Definition for WMPP _ALR.1 (EX)

For the TOE described in this ST it was necessary to define a new family (WMPP_ALR) that addresses rules which define the generation of alerts, messages, as well as the disposition of events. This family contains the component as shown in Figure 6 below.

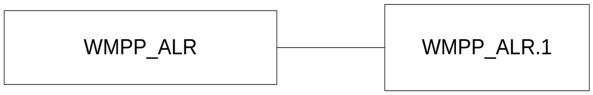

Figure 6: WMPP_ALR Component Leveling

5.2.1. Data Alarms (WMPP _ALR.1 (EX))

WMPP_ALR.1.1 Defines groups or rules as well as rules for the generation of events using one or more notification mechanisms. This component may include:

- Display alarm information to the administrator console
- Send alarm information to administrators using email
- Execute a command

- Execute a script

in response to the operation performed or event.

5.2.2. Dependencies:

- None

5.2.3. Management:

- None

5.3. Definition WMPP_STG.1 (EX)

For the TOE described in this ST it is necessary that the WMPP be able to handle the case in which the system has run out of storage capacity. In order to do this it was necessary that we define a new family (WMPP_STG). This family contains the components as shown in the figure below.

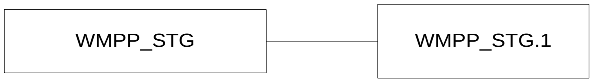

Figure 7: WMPP_STG Component Leveling

5.3.1. Data Loss Prevention (WMPP_STG.1 (EX))

WMPP_STG.1.1 This component requires an action be taken with respect to the collection of System data and the blocking of all transactions and generating a message or alarm if the storage capacity has been reached.

5.3.2. Dependency:

- WMAP_ALR.1.1

5.3.3. Management:

- None

6. IT Security Requirements (ASE_REQ)

This section defines the security functional requirements for the TOE as well as the security assurance requirements against which the TOE has been evaluated. All of the requirements have been copied from version 3.1 of the applicable Common Criteria documents, with the exception of the explicitly stated Security Functional Requirements.

6.1. TOE Security Functional Requirements

Class	Component
FAU: Security Audit	FAU_ARP.1: Security alarms
	FAU_GEN.1: Audit data generation
	FAU_SAA.1: Potential violation analysis
	FAU_SAR.1: Audit review
	FAU_STG.1: Protected audit trail storage
FDP: User Data Protection	FDP_ACC.1: Subset access control
	FDP_ACF.1: Security attribute based access control
FIA: Identification and Authentication	FIA_ATD.1: User attribute definition
FMT: Security management	FMT_MOF.1: Management of security functions behavior
	FMT_MSA.1: Management of Security Attributes
	FMT_MSA.3: Static Attribute Initialization
	FMT_MTD.1: Management of TSF data
	FMT_SMF.1: Specification of management Functions
	FMT_SMR.1: Security roles
WMPP: Windows Management Performance Proxy	WMPP_ADM.1(EX): Data Review
	WMPP_ALR.1(EX): Data Alarms
	WMPP_STG.1(EX): Data Loss Prevention

Table 7: TOE Security Functional Requirements

6.1.1. Security Audit (FAU)

6.1.1.1. Security alarms (FAU_ARP.1)

FAU_ARP.1.1 The TSF shall take [**post a message, block the transaction, and generate a log entry**] upon detection of a potential security violation.

6.1.1.2. Audit data generation (FAU_GEN.1)

FAU_GEN.1.1 The TSF shall be able to generate an audit record of the following auditable events:

a) Start-up and shutdown of the audit functions;
b) All auditable events for the [*detailed*] level of audit; and
c) [**All auditable events listed in Table 9**]…

FAU_GEN.1.2 The TSF shall record within each audit record at least the following information:

a) Date and time of the event, type of event, subject identity ~~(if applicable),~~ and the outcome (success or failure) of the event; and
b) For each audit event type, based on the auditable event definitions of the functional components included in the ~~PP/~~ST, [**All auditable events listed in Table 9**].

FAU_ARP.1	The TOE allows access to functions based on privileges provided to Administrators, AM Users, or Agents.
FAU_GEN.1	The TOE generates audit data for ALL jobs attempted and executed through GUI/UI (Console subsystem) or

	the Agent communication path.
FAU_SAA.1	The TOE provides functions to analyze audit events (all transactions attempted and executed) and provide trends as part of the GUI/UI (Console) analysis reporting subsystem.
FAU_SAR.1	The TOE provides event audit review for all attempted and executed jobs as part of the GUI / UI (Console subsystem).
FAU_STG.1	The TOE stores audit event information for all attempted and executed jobs in a protected area in the QDB.
FDP_ACC.1	The TOE generates audit information regarding changes to access jobs.
FDP_ACF.1	The TOE shall enforce access control to Audit records (containing all attempted and executed transactions) and prevent unauthorized deletion or modification of audit records.
FMT_MOF.1	The TOE shall generate audit information regarding enabling or disabling Job / Script Management
FMT_MSA.1	The TOE shall generate audit information regarding changes to jobs.
FMT_MTD.1	The TOE shall generate audit information for changes to job configuration data and reports.
FMT_SMF.1	The TOE shall generate audit information for addition of jobs.
WMPP_ADM.1(EX)	The TOE provides audit record information around the results of jobs...
WMPP_ALR.1(EX)	The TOE provides the ability to generate audit information for messages or alarms.
WMPP_STG.1(EX)	The TOE provides the ability to block transactions when audit storage capacity has been reached.

Table 8: Auditable Events

6.1.1.3. Potential violation analysis (FAU_SAA.1)

FAU_SAA.1.1 The TSF shall be able to apply a set of rules in monitoring the audited events and based upon these rules indicate a potential violation of the enforcement of the SFRs.

FAU_SAA.1.2 The TSF shall enforce the following rules for monitoring audited events:
a) Accumulation or combination of [**no such events specified**] known to indicate a potential security violation;
b) [**all transactions performed by Administrators, AM Users or AM Agents**].

6.1.1.4. Audit review (FAU_SAR.1)

FAU_SAR.1.1 The TSF shall provide [**Administrators**] with the capability to read [**all audit information**] from the audit records.

FAU_SAR.1.2 The TSF shall provide the audit records in a manner suitable for the user to interpret the information.

6.1.1.5. Protected audit trail storage (FAU_STG.1)

FAU_STG.1.1 The TSF shall protect the stored audit records in the audit trail from unauthorized deletion.

FAU_STG.1.2 The TSF shall be able to [*prevent*] unauthorized modifications to the stored audit records in the audit trail.

6.1.2. User Data Protection (FDP)

6.1.2.1. Subset access control (FDP_ACC.1)

FDP_ACC.1.1: The TSF shall enforce the [**access control**] on [**All AM Components for Read, write, modify, or execute access to Administrators, AM Users , AM Agents**]

6.1.2.2. Security attribute based access control (FDP_ACF.1)

FDP_ACF.1.1 The TSF shall enforce the [**access control**] to objects based on the following: [**Membership in the:**

Administrators group,
AM Users,
or AM Agents

for Read, Write, Execute access to all AM objects].

FDP_ACF.1.2 The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: [**user execution based on membership in the Administrators group, AM Users, or AM Agents**]*.*

FDP_ACF.1.3 The TSF shall explicitly authorize access of subjects to objects based on the following additional rules: [**none**].

FDP_ACF.1.4 The TSF shall explicitly deny access of subjects to objects based on the following additional rules: [**Users not in the Administrators group, AM users without any privileges specified in Appendix A.**].

6.1.3. Identification and Authentication (FIA)

6.1.3.1. User attribute definition (FIA_ATD.1)

FIA_ATD.1.1 The TSF shall maintain the following list of security attributes belonging to individual ~~users~~ **roles**: **[authorizations]**.

6.1.4. Security management (FMT)

6.1.4.1. Management of security functions behavior (FMT_MOF.1)

FMT_MOF.1.1 The TSF shall restrict the ability to [*enable and disable*] the functions **[that enable Job / Script Management**] to [**Administrators or AM Users with privileges in Appendix A**]

6.1.4.2. Management of Security Attributes (FMT_MSA.1)

FMT_MSA.1.1 The TSF shall enforce the [**Access Controls**] to restrict the ability to [*modify, **add,** or delete*] the security attributes [**privileges and groups of privileges**] to [**Administrators**].

6.1.4.3. Static attribute initialization (FMT_MSA.3)

FMT_MSA.3.1 The TSF shall enforce the [**Access Control**] to provide [*restrictive*] default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2 The TSF shall allow the [**Administrators, AM Users**] to specify alternative initial values to override the default values when an object or information is created.

6.1.4.4. Management of TSF data (FMT_MTD.1)

FMT_MTD.1.1 The TSF shall restrict the ability to [*modify*] the [**configuration data and**

reports] to [**Administrators or AM Users with the appropriate privileges**].

6.1.4.5. Specification of Management Functions (FMT_SMF.1)

FMT_SMF.1.1 The TSF shall be capable of performing the following security management functions: [
Add Additional AM Users,
Modify the behavior of AM Users
Modify the behavior of operation events
Query collected transaction log and generate reports]

6.1.4.6. Security Roles (FMT_SMR.1)

FMT_SMR.1.1 The TSF shall maintain the roles [**Administrators, AM users, and AM Agents**].

FMT_SMR.1.2 The TSF shall be able to associate users with roles.

6.1.5. Windows Management Administrative Proxy (WMPP)

6.1.5.1. Data Review (WMPP_ADM.1 (EX))

WMPP_ADM.1.1 The TSF shall provide Administrators the capability to delegate to authorized users the ability to issue administrative commands and changes.

WMPP _ADM.1.2 The TSF shall provide Administrators the ability to delegate to authorized users a group or set of abilities.

6.1.5.2. Data Alarms (WMPP_ALR.1 (EX))

WMPP _ALR.1.1 The TSF shall generate an alarm using one or more of the following notification mechanisms:
Display alarm information to the console

- Send alarm information to Administrators or AM Users using email
- Execute a command
- Execute a script in response to one or more of the following rule types:
  Event rules

Application note: Scripts and commands can be used to support notification mechanisms for which there is no built-in support.

6.1.5.3. Data Loss Prevention (WMPP_STG.1 (EX))

WMPP_STG.1.1 The TSF shall abort the attempted command, display a message if the storage capacity has been reached. (EX)

6.2. Security Assurance Requirements

This section defines the assurance requirements for the TOE. The TOE assurance requirements are taken from the CC v3.1 Release 3, Part 3. The TOE consists of the requirements specified for EAL2 of assurance augmented by Basic Flaw Remediation (ALC_FLR.1). The following table summarizes the requirements.

Assurance Class	Assurance Components	
ADV: Development	ADV_ARC.1	Security architecture description
	ADV_FSP.2	Security –enforcing functional specification
	ADV_TDS.1	Basic design
AGD Guidance documents	AGD_OPE.1	Operational user guidance
	AGD_PRE.1	Preparative procedures
ALC: Life-cycle support	ALC_CMC.2	Use of a CM system

	ALC_CMS.2	Parts of the TOE CM coverage
	ALC_DEL.1	Delivery procedures
	ALC_FLR.1	Flaw Remediation Procedures
ASE: Security Target evaluation	ASE_CCL	Conformance claims
	ASE_ECD.1	Extended components definition
	ASE_INT.1	Introduction
	ASE_OBJ.2	Security objectives
	ASE_REQ.2	Derived security requirements
	ASE_SPD.1	Security problem definition
	ASE_TSS.1	TOE Summary specification
ATE: Tests	ATE_COV.1	Evidence of coverage
	ATE_FUN.1	Functional testing
	ATE_IND.2	Independent testing - sample
AVA: Vulnerability Assessment	AVA_VAN.2	Vulnerability analysis

Table 9: Security Assurance Requirements

7. TOE Summary Specification (ASE_TSS)

This chapter describes the security functions.

7.1. Security Audit

The NetIQ AppManager product provides the ability to make changes to application or system configurations, monitor applications or systems performance needs, and generate events and alerts based on predefined parameters. All access and activities performed by the Administrators or AM Users is logged.

The TOE generates audit records for Security Relevant events. The table of the audit events generated by the TOE is provided in Table 9 - Auditable Events...

Access to the Audit facility is restricted to Administrators.

The Security Audit function is designed to satisfy the following security functional requirements of FAU_GEN.1.

7.2. User Data Protection

The NetIQ AppManager product provides the ability to make changes to application or system configurations, monitor applications or systems performance needs, and generate events and alerts based on predefined parameters. The AppManager product is protected by enforcing the privileges associated to Administrators, AM Users, or Agents. These privileges are associated in the following ways:

- by virtue of being an Administrator (i.e. membership in the Administrators group),

- having privileges as described in Appendix A

- being in the AM Users group

The User Data Protection function is designed to satisfy the following security functional requirements:

FDP_ACC.1 The TOE allows access to information by enforcing user privileges as defined by:

- membership in the Administrator's or AM Users group
- users with privileges specified in Appendix A
- Agents with credentials in the QDB

FDP_ACF.1 The TOE enforces access to functions based on the user privileges as defined by

- Membership in the Administrator's or AM Users group
- Users with privileges specified in Appendix A
- Execution of jobs (knowledge scripts + additional details) is a privilege in Appendix A and B
- Importing and exporting knowledge scripts are privileges in Appendix A and B
- Agents with credentials in the QDB

FIA_ATD.1 The TOE will maintain a list of security attributes belonging to AM Users and Agents

WMPP_ADM.1.1 The TOE defines mechanisms for Administrators to delegate privileges to individuals.

WMPP_ADM.1.2 The TOE defines mechanisms for Administrators to delegate privileges to users or groups of users an ability or set of abilities.

7.3. Identification and Authentication

NetIQ AppManager provides user interfaces that Administrators may use to define roles and delegate responsibilities. These roles may be assigned to users, groups of users, machines (agents) or groups of machines (agents). The TOE maintains a list of authorizations associated with each user, group, or agent.

If the user has been successfully identified and authenticated by the environment the Console provides access to its interfaces according to authorization data stored in the Data Repository. Authorization data maintained by the TOE, for each role that the TOE recognizes is used to determine the functions that a user possessing a given role (i.e. privileges afforded by the TOE) may perform.

The TOE recognizes the following groups, which correspond to TOE roles:

Administrator
AM Users
AM Agents

The TOE also recognizes users that have privileges within the TOE according to the table below.

Deployment Permissions		Privileges
	Rules	copy, delete, create, modify, enable or disable, import
	Tasks	change credentials for deployment tasks, reject or delete, configure deployment, change schedule for deployment tasks, approve tasks
	Packages	delete packages, Allowed to check in packages
Management Group Permissions		Privileges
	Custom Property	create or update, delete existing
	Job	start/stop/close existing jobs, delete existing jobs, update job properties, create new jobs create/modify a job view, delete a job view, access a job view
	Knowledge Script	propagate Knowledge Script properties to a job or to a Knowledge Script Group member, check Knowledge Scripts into a repository, update Knowledge Script properties, delete existing Knowledge Scripts, create a new Knowledge Script Group, copy existing Knowledge Script, check existing Knowledge Scripts out of a repository, delete a Knowledge Script view, create/modify a Knowledge Script view, access a Knowledge Script view
	Server	enable/disable a computer's maintenance mode, delete servers, create/modify a server view, delete a server view, access a server view
	Event	delete existing events, acknowledge or close existing events, update comments for existing events, create/modify an event view, access an event view, delete an event view
	Monitoring Policy	start/stop/close existing monitoring policy jobs, delete policy, create policy
	Management Group Administration	modify security properties, modify policy properties, modify general properties, modify members properties, create/modify management groups
	Service Map	access a service map view, delete a service map view, create/modify a service map view
General Permissions		Privileges
	Computer	add a computer to a repository

Table 10: Privileges

Finally the TOE recognizes machines (Agents), or groups of machines (Agents) for the purpose of sending & receiving information.

The Identification and authentication function is designed to satisfy the following security functional requirements:

FIA_ATD.1:	The TOE maintains authorization information that determines which TOE functions a role may perform.
FMT_SMR.1:	The TOE allows for the provisioning of different groups prior to allowing access.

7.4. Security Management

The NetIQ AppManager application includes the following components:

- Console
  - Control Center Console
  - Operator Console
- AppManager Repository
  - Control Center Database (CCDB)
  - NetIQ Database (QDB)
- Management Server (MS)
  - Task Scheduler (NQAMTS)
  - Control Center Queue Service (CQS)
- Deployment Server
  - Control Center Deployment Web Server (CCDWS)
  - Control Center Deployment Service
- AppManager Agents (Agents)

7.4.1. Console:

The *Console* contains the Control Center Console and the Operator Console. Both consoles can only be executed by users that are granted privileges on the machine.

While anyone can execute the Console applications, only users with privileges specified in the TOE can perform any actions.

As a default the following group has all permissions

- Administrator

Users with privileges (listed in table 9 – above) can perform the actions as described.

The security management function is designed to satisfy the following security functional requirements:

FMT_MOF.1:	The TOE restricts the ability to manage WMPP settings to authorized administrators or users with privileges specified in Appendix A.
FMT_MSA.1	The TOE shall enforce access controls that restrict the ability to modify, add, or delete security attributes or privileges and groups of privileges to Administrators
FMT_MSA.3	The TOE provides a default set of privileges as well as the ability for Administrators to modify the default.
FMT_MTD.1:	The TOE restricts the ability to modify configuration data and generated reports to Administrators or AM users with the appropriate privileges.
FMT_SMF.1:	The TOE provides authorized administrators with the ability to add additional AM users, modify the behavior of AM Users, modify the behavior of operation events, query collected transaction logs and generate reports.
FMT_SMR.1:	The TOE allows for the provisioning of different groups prior to allowing access.
WMPP_ALR.1(EX)	The TOE provides the ability to generate messages or alarms.

WMPP_STG.1(EX) The TOE provides the ability to block transactions when storage capacity has been reached.

7.4.2. AppManager Repository:

Users gain access to the repository via the Console. The console can rely on either AD or SQL authentication. When the user credentials are presented to the Repository they are associated with a set of Agents as well as functions they may perform on the Agents. Based on the information provided by the AppManager Repository the console can be used to:

- stop / start jobs
- create new jobs
- get data
- define access
- create groups of Agents (machines)
- create new agents (Agents)

The security management function is designed to satisfy the following security functional requirements:

FMT_MOF.1: The TOE restricts the ability to manage WMPP settings to authorized administrators or users with privileges specified in Appendix A.

FMT_MTD.1: The TOE restricts the ability to modify configuration data and reports to AM Administrators or AM users with the appropriate privileges.

FMT_SMF.1: The TOE provides authorized administrators with the ability to add additional AM users, modify the behavior of AM Users, modify the behavior of operation events, query collected transaction logs and generate reports.

FMT_SMR.1: The TOE allows for the provisioning of different groups prior to allowing access.

7.4.3. Management Server (MS)

The Management Server is used to post jobs to the Managed Client from the Data Repository and receive /forward data back to the Data Repository.
The security management function is designed to satisfy the following security functional requirements:

WMPP_ALR.1(EX) The TOE provides the ability to generate messages or alarms.

WMPP_STG.1(EX) The TOE provides the ability to block transactions when storage capacity has been reached.

7.4.4. Deployment Server (DS)

The Security management function is designed to satisfy the following security functional requirements:

FMT_MOF.1: The TOE restricts the ability to manage WMPP settings to authorized administrators or users with privileges specified in Appendix A.

FMT_MTD.1: The TOE restricts the ability to modify configuration data and reports to AM Administrators or AM users with the appropriate privileges.

7.4.5. AppManager Agent[7]

The Agent (Managed Client) gathers information based on the contents of the jobs it receives, and provides it back to the Management Server.

The security management function is designed to satisfy the following security functional requirements:

[7] Configured with FIPS and OpenSSL

WMPP_ALR.1(EX)	The TOE provides the ability to generate messages or alarms.
WMPP_STG.1(EX)	The TOE provides the ability to block transactions when storage capacity has been reached.

8. Appendix A

8.1. Administrators Group:

Can create additional administrators or users with privileges.

8.2. Users defined permissions and permission sets:

Permission Class	Realm	Rule
Deployment Permissions	Deployment Packages	Allowed to check in deployment packages
		Allowed to delete deployment packages
	Deployment Rules	Allowed to copy deployment rules
		Allowed to create deployment rules
		Allowed to delete deployment rules
		Allowed to enable and disable deployment rules
		Allowed to import deployment rules
		Allowed to modify deployment rules
	Deployment Tasks	Allowed to approve deployment tasks
		Allowed to change credentials for deployment tasks
		Allowed to change schedules for deployment tasks
		Allowed to configure deployment tasks
		Allowed to delete deployment tasks
		Allowed to reject deployment tasks
General Permissions	Computer	Allowed to add computers to repositories
Management Group and View Permissions	Chart	Allowed to access chart views
		Allowed to delete data streams
		Allowed to modify chart views
	Custom Property	Allowed to create custom properties
		Allowed to delete custom properties
		Allowed to delete custom property definitions
		Allowed to update custom properties
	Event	Allowed to access event views
		Allowed to acknowledge and close events
		Allowed to create and modify event views
		Allowed to delete event views
		Allowed to delete events
		Allowed to modify event comments
	Job	Allowed to access job views
		Allowed to add child jobs
		Allowed to close jobs
		Allowed to create and modify job views
		Allowed to create jobs
		Allowed to delete job views
		Allowed to delete jobs
		Allowed to modify job properties

Permission Class	Realm	Rule
		Allowed to start jobs
		Allowed to stop jobs
	Knowledge Script	Allowed to access knowledge script views
		Allowed to check knowledge scripts and knowledge script groups into repositories
		Allowed to check knowledge scripts and knowledge script groups out of repositories
		Allowed to copy knowledge scripts and knowledge script groups
		Allowed to create and modify knowledge script views
		Allowed to create knowledge script groups
		Allowed to delete knowledge script views
		Allowed to delete knowledge scripts and knowledge script groups
		Allowed to modify knowledge script and knowledge script group properties
		Allowed to propagate knowledge script properties to jobs and knowledge script group members
		Allowed to change management group and folder general properties
		Allowed to change management group members
		Allowed to change management group policies
		Allowed to change management group security permissions
		Allowed to create and modify management groups and folders
		Allowed to move management groups and folders
	Monitoring Policy	Allowed to close monitoring policy jobs
		Allowed to create monitoring policies
		Allowed to delete monitoring policies
		Allowed to start monitoring policy jobs
		Allowed to stop monitoring policy jobs
		Allowed to update monitoring policies
	Server	Allowed to access server views
		Allowed to create and modify server views
		Allowed to delete server views
		Allowed to delete servers
		Allowed to put servers into/take servers out of the maintenance mode
	Service Map	Allowed to access service maps
		Allowed to create and modify service maps
		Allowed to delete service maps

9. Appendix B – Explicit privilege list

Privilege	Privilege	Privilege
1. Allowed to check in deployment packages	Allowed to delete deployment packages	Allowed to copy deployment rules
2. Allowed to create deployment rules	Allowed to delete deployment rules	Allowed to enable and disable deployment rules
3. Allowed to import deployment rules	Allowed to modify deployment rules	Allowed to approve deployment tasks
4. Allowed to change credentials for deployment tasks	Allowed to change schedules for deployment tasks	Allowed to configure deployment tasks
5. Allowed to delete deployment tasks	Allowed to reject deployment tasks	Allowed to add computers to repositories
6. Allowed to access chart views	Allowed to delete data streams	Allowed to modify chart views
7. Allowed to create custom properties	Allowed to delete custom properties	Allowed to delete custom property definitions
8. Allowed to update custom properties	Allowed to access event views	Allowed to acknowledge and close events
9. Allowed to create and modify event views	Allowed to delete event views	Allowed to delete events
10. Allowed to modify event comments	Allowed to access job views	Allowed to add child jobs
11. Allowed to close jobs	Allowed to create and modify job views	Allowed to create jobs
12. Allowed to delete job views	Allowed to delete jobs	Allowed to modify job properties
13. Allowed to start jobs	Allowed to stop jobs	Allowed to access knowledge script views
14. Allowed to check knowledge scripts and knowledge script groups into repositories	Allowed to check knowledge scripts and knowledge script groups out of repositories	Allowed to copy knowledge scripts and knowledge script groups
15. Allowed to create and modify knowledge script views	Allowed to create knowledge script groups	Allowed to delete knowledge script views
16. Allowed to delete knowledge scripts and knowledge script groups	Allowed to modify knowledge script and knowledge script group properties	Allowed to propagate knowledge script properties to jobs and knowledge script group members
17. Allowed to change management group and folder general properties	Allowed to change management group members	Allowed to change management group policies
18. Allowed to change management group security permissions	Allowed to create and modify management groups and folders	Allowed to move management groups and folders
19. Allowed to close monitoring policy jobs	Allowed to create monitoring policies	Allowed to delete monitoring policies
20. Allowed to start monitoring policy jobs	Allowed to stop monitoring policy jobs	Allowed to update monitoring policies
21. Allowed to access server views	Allowed to create and modify server views	Allowed to delete server views
22. Allowed to delete servers	Allowed to put servers into/take servers out of the maintenance mode	Allowed to access service maps
23. Allowed to create and modify service maps	Allowed to delete service maps	